X.509 Defect Report:

Policy Mapping

Santosh Chokhani

chokhani@cygnacom.com

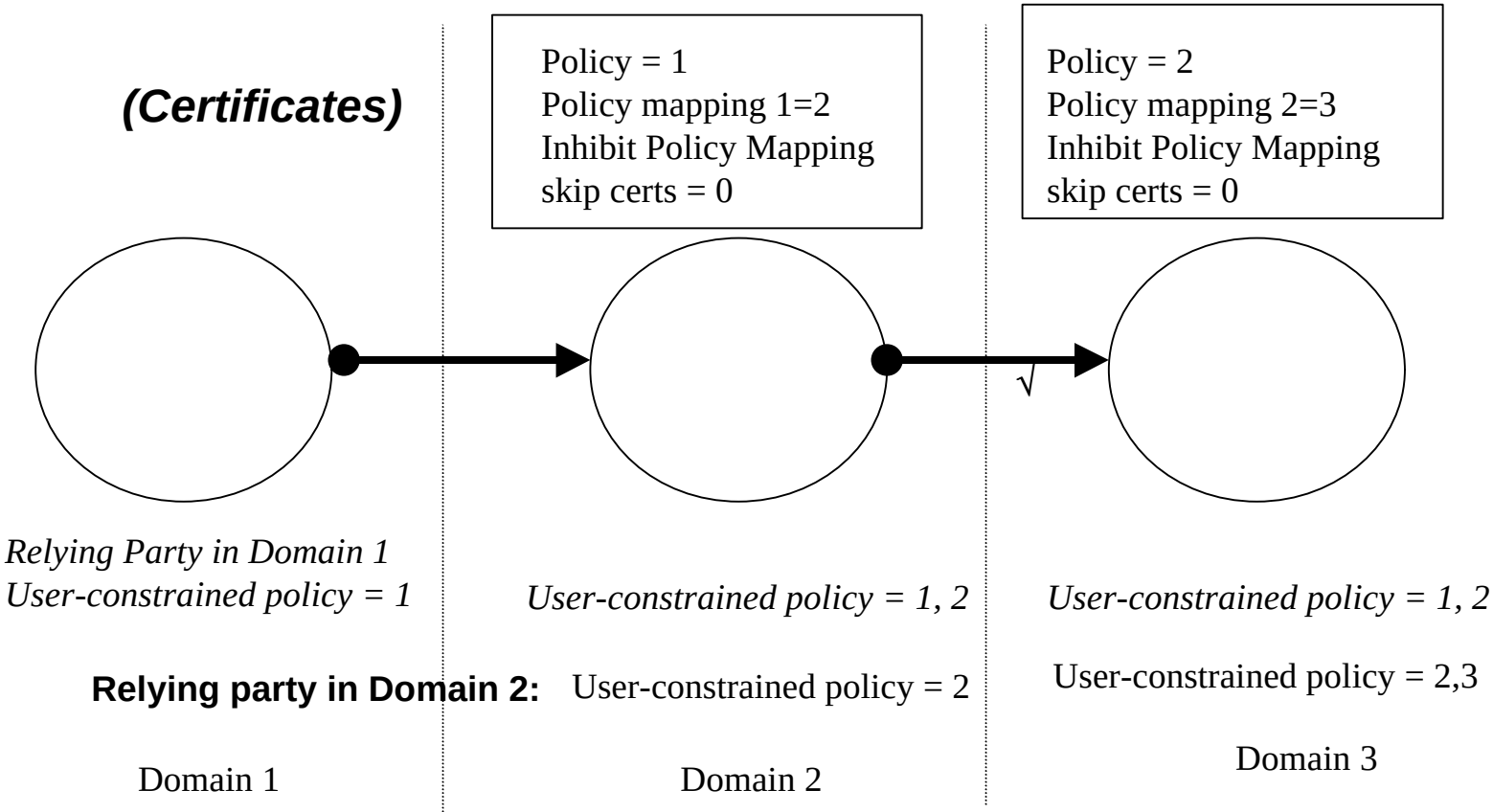
CygnaCom Solutions, Inc. ◆ Suite 100W, 7927 Jones Branch Drive, McLean, VA 22102 ◆ (703) 848-0883

Policy Mapping Processing

- **X.509 Amendment, Section 12.4.3:**
  - Check for a valid certificate policy first
  - Perform policy mapping next
- **Implications**
  - Issuer must assert issuer domain policy in the subject certificate
- **Problem**
  - Asserting issuer domain policy does not truly inhibit policy mapping when a domain intends to inhibit policy mapping

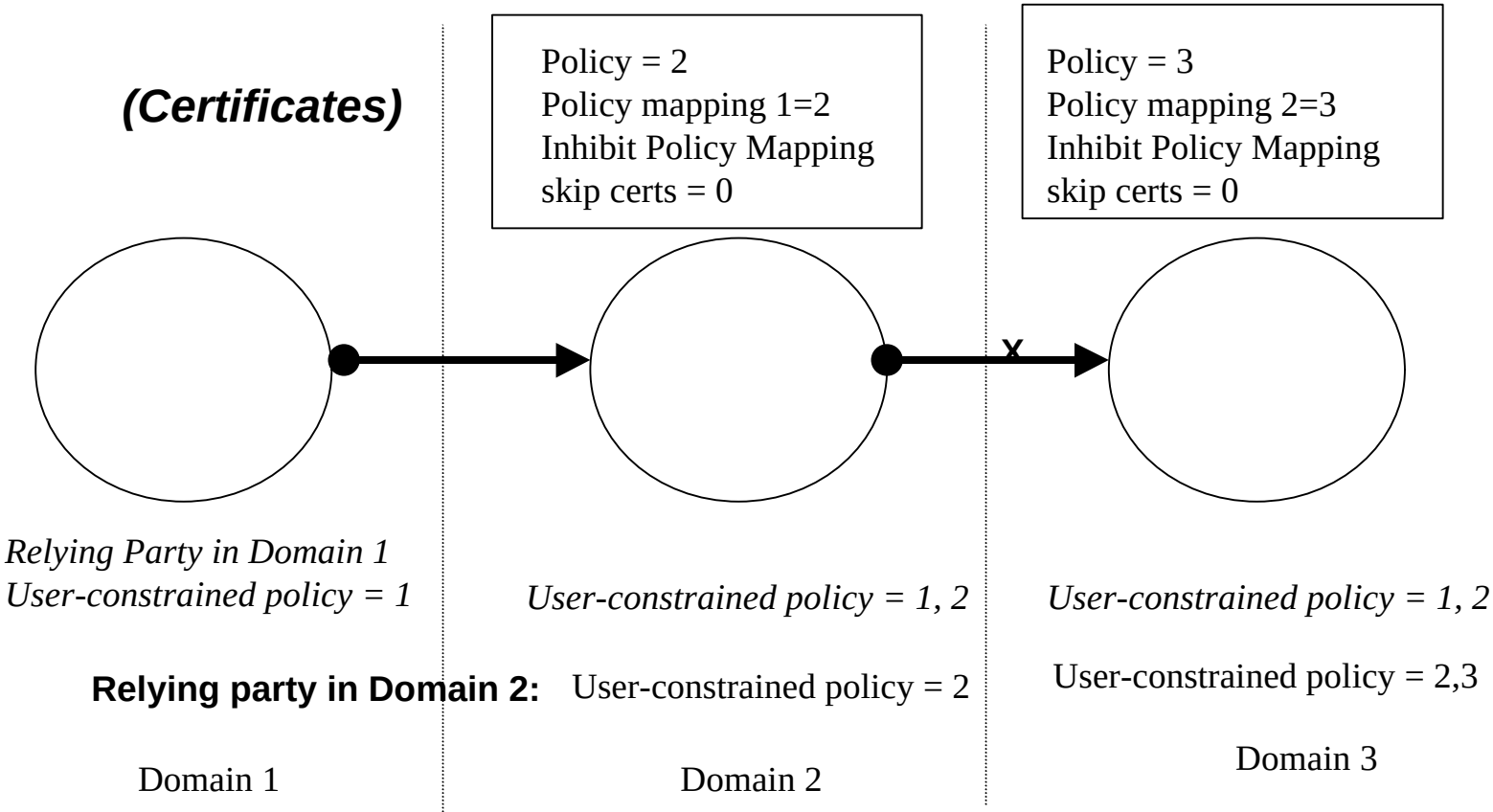
CYGNACOM SOLUTIONS

Current Approach to Policy Mapping in X.509



CYGNACOM SOLUTIONS

Proposed Approach to Policy Mapping in X.509



CYGNACOM SOLUTIONS

Proposed Solution

- **Add advisory in X.509 Certificate policy extension (Section 12.2.2.6),**
  - Issuer should asserts subject domain policy in the certificate policies extension
- **Change X.509 Amendment, Section 12.4.3:**
  - Perform policy mapping first
  - Check for a valid certificate policy after performing policy mapping

CYGNACOM SOLUTIONS

Specific Defect Report Solution (1/2)

Add the following to the certificate policy extension section (section 12.2.2.6) “If the subject of the certificate is a CA in another domain, the policy(s) asserted shall be those of the subject CA’s domain.”

Delete the following from item e (“If policy-mapping-inhibit-indicator is not set:..”) in path validation section, 12.4.3:

- **process any policy mapping extension with respect to policies in the user-constrained-policy-set and add appropriate policy identifiers to the user-constrained-policy-set .**
- **process any policy mapping extension with respect to policies in the authority-constrained-policy-set and add appropriate policy identifiers to the authority-constrained-policy-set .**

CYGNACOM SOLUTIONS

Specific Defect Report Solution (1/2)

Add the following to the list of check just prior to item “c” check in path validation section, 12.4.3.

“If policy-mapping-inhibit-indicator is not set:.

- **process any policy mapping extension with respect to policies in the user-constrained-policy-set and add appropriate policy identifiers to the user-constrained-policy-set .**
- **process any policy mapping extension with respect to policies in the authority-constrained-policy-set and add appropriate policy identifiers to the authority-constrained-policy-set .”**

CYGNACOM SOLUTIONS